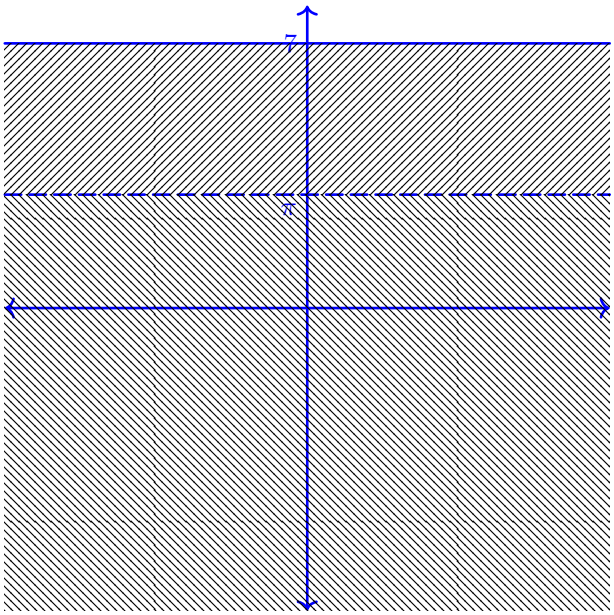
TMA 05 202xJ

TMA 05

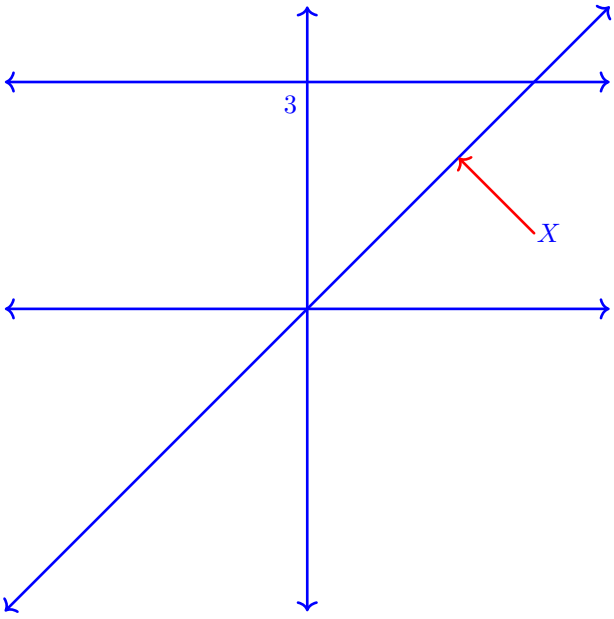
Solution to Question 7 – 10 marks

(a) W An example of a sketch (both shaded parts comprise W)



Description: there is a horizontal solid line going through $y = 7$ and a horizontal dashed line going through $y = \pi$. Between the $y = 7$ line and the $y = \pi$ lines there is one kind of shading and below $y = \pi$ there is a different kind of shading.

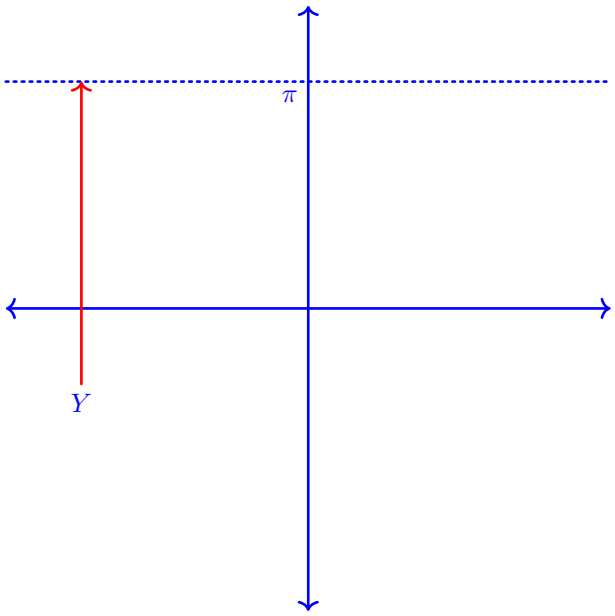
X An example of a sketch



Description: There is a solid horizontal line through $y = 3$ and a solid line with gradient 1 through the origin.

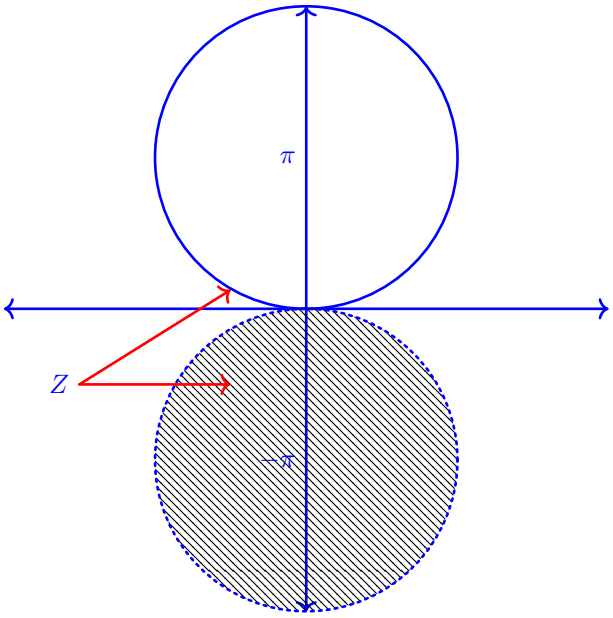
Y An example of a sketch

Copyright © 2020 The Open University



Description: there is a horizontal dotted line through $y = \pi$.

Z An example of a sketch



Description: there are two circles, vertically one above the other and just touching. The top one is a solid, unshaded circle with centre $(0, \pi)$ and radius π. The lower one is dotted and shaded with centre $(0, -\pi)$ and radius π.

(b) W Disconnected

X Connected

Y Disconnected

Z Connected

A disconnection for W is
$\{(x, y) \in \mathbb{R}^2 : y < \pi\} \cup \{(x, y) \in \mathbb{R}^2 : y > \pi \text{ and } y \leq 7\}$.

There are many disconnections for Y (since it is totally disconnected). An example is $\{(q, \pi) : q \in \mathbb{Q} \text{ and } q < \pi\} \cup \{(q, \pi) : q \in \mathbb{Q} \text{ and } q > \pi\}$

Chapter 21, Exercise 3.1 and Exercise 3.10.

Solution to Question 8 – 10 marks

(a) Since $q = (n+1)/p$ is an integer by our assumptions, we have $1 + n = pq$; another factorisation (as in the Solution to Exercise 2.13(b) of Chapter 17) is $1 + n = (1 + \sqrt{-n})(1 - \sqrt{-n})$.

If p was a prime in R, then p would have to divide one of $1 + \sqrt{-n}$, $1 - \sqrt{-n}$.

Thus, we would have $p(r + s\sqrt{-n}) = (1 \pm \sqrt{-n})$ for some $r, s \in \mathbb{Z}$; in particular, p would have to divide 1, a contradiction.

We conclude that p cannot be a prime in R.

Solution to Exercise 2.13(b) of Chapter 17

(b) Following the hint, since $n \geq 3$, n is odd, and p divides $n + 1$, we have $n > p$.

Suppose that $r^2 + ns^2 = p$ for some $r, s \in \mathbb{Z}$. If $s \neq 0$, then $r^2 + ns^2 \geq n > p$, a contradiction.

It follows that $s = 0$, and so $r^2 = p$, a contradiction again.

Consequently, there is no element of R with norm equal to p.

(c) Suppose that p is reducible in R, that is,

$$p = (r + s\sqrt{-n})(u + v\sqrt{-n}) \quad \text{for some} \quad r, s, u, v \in \mathbb{Z}\ .$$

Taking norms, we obtain $p^2 = (r^2 + ns^2)(u^2 + nv^2)$.

This means that either $r^2 + ns^2 = u^2 + nv^2 = p$ (which is ruled out by the result of (b)), or one of $r^2 + ns^2$, $u^2 + nv^2$ is equal to 1.

But then $r = \pm 1$, $s = 0$ or $u = \pm 1$, $v = 0$. When combined with the displayed equation, the first possibility gives $u = \pm p$, $v = 0$ and the second possibility yields $r = \pm p$, $s = 0$. It follows that p is irreducible in R.

Solution to Question 9 – 8 marks

(a) The minimal polynomial for $\sqrt[3]{7}$ is $x^3 - 7$; it is irreducible over $\mathbb{Q}$, because it has degree 3 and does not have a rational root. (Another way to argue is to use Eisenstein's criterion.) It follows that $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$.

The minimal polynomial for $\sqrt[4]{7}$ is $x^4 - 7$; it is irreducible by Eisenstein's criterion Theorem 4.15 of Chapter 11, since the prime $p = 7$ divides all the coefficients of the polynomial except for the leading one, and p^2 does not divide the constant term. It follows that $[\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] = 4$.

(b) If $\sqrt[3]{7} \in \mathbb{Q}(\sqrt[4]{7})$, then $\mathbb{Q}(\sqrt[3]{7})$ would have to be a subfield of $\mathbb{Q}(\sqrt[4]{7})$. But then, by the KLM Theorem Theorem 2.29 of Chapter 18, the degree $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}]$ would have to be a divisor of the degree $[\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}]$, a contradiction by the result of part (a).

(c) By the results of parts (a) and (b), the minimal polynomial of $\sqrt[3]{7}$ over $\mathbb{Q}(\sqrt[4]{7})$ is still $x^3 - 7$ and so $[\mathbb{Q}(\sqrt[3]{7}, \sqrt[4]{7}) : \mathbb{Q}(\sqrt[4]{7})] = 3$.

Since $[\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] = 4$, the KLM Theorem gives $[\mathbb{Q}(\sqrt[3]{7}, \sqrt[4]{7}) : \mathbb{Q}] = 12$.

(d) Since $\sqrt[3]{7} \cdot \sqrt[4]{7} = (\sqrt[12]{7})^7$, or, alternatively, $7^{\frac{1}{3}} \cdot 7^{\frac{1}{4}} = (7^{\frac{1}{12}})^7$, we have $\mathbb{Q}(\sqrt[3]{7} \cdot \sqrt[4]{7}) \subseteq \mathbb{Q}(\sqrt[12]{7})$ and $\mathbb{Q}(\sqrt[12]{7}) \subseteq \mathbb{Q}(\sqrt[3]{7} \cdot \sqrt[4]{7})$; hence $\mathbb{Q}(\sqrt[3]{7} \cdot \sqrt[4]{7}) = \mathbb{Q}(\sqrt[12]{7})$.

Certainly $\mathbb{Q}(\sqrt[3]{7}, \sqrt[4]{7}) \subset \mathbb{Q}(\sqrt[12]{7})$, and since $\sqrt[3]{7} \cdot \sqrt[4]{7} \in \mathbb{Q}(\sqrt[3]{7}, \sqrt[4]{7})$ we also have $\mathbb{Q}(\sqrt[3]{7}, \sqrt[4]{7}) = \mathbb{Q}(\sqrt[3]{7} \cdot \sqrt[4]{7})$.

Solution to Question 10 – 11 marks

(a) We have

$$\omega^3 = \omega^2\omega = (2+3\omega)\omega = 2\omega + 3(2+3\omega) = 1+\omega.$$

Similarly,

$$\omega^6 = (1+\omega)^2 = 1 + 2\omega + (2+3\omega) = 3.$$

(b) To show that ω is a primitive element, we need to demonstrate that $\omega^i \neq 1$ for any positive divisor i of 24 such that $i < 24$.

Since $\omega^{12} = 3^2 = -1$ and $\omega^8 = 3\omega^2 \neq 1$, we have $\omega^i \neq 1$ for $i \in \{3, 6, 12\}$ and for $i \in \{2, 4, 8\}$. Hence ω is a primitive element of F.

(c) Following the second method of Worked Exercises 3.10(b) and 3.11(c) of Chapter 18, we determine $a, b \in \mathbb{Z}_5$ satisfying $\omega(a+b\omega) = 1 = 1 + 0\cdot\omega$. Using $\omega^2 = 2 + 3\omega$ the first equation simplifies (after rearranging terms) to $2b + (a+3b)\omega = 1$. This gives $2b = 1$, that is, $b = 3 = -2$ in $\mathbb{Z}_5$, and from $a + 3b = 0$ we have $a = 1$. It follows that $\omega^{-1} = 1 + 3\omega = 1 - 2\omega$.

Worked Exercises 3.10(b) and 3.11(c) of Chapter 18

(d) By Corollary 3.5 of Chapter 18 the primitive elements of F are precisely the powers ω^i for positive integers i smaller than $5^2 - 1 = 24$ and relatively prime to 24. In our case, it is the 8 values of $i \in \{1, 5, 7, 11, 13, 17, 19, 23\}$.

Using $\omega^6 = 3$, $\omega^{12} = -1$ and $\omega^{-1} = \omega^{23} = 1 - 2\omega$, and knowing $\omega^1 = \omega$ and $\omega^{-1} = \omega^{23}$, for the remaining 6 powers ω^i we successively obtain:

$$\begin{aligned}
\omega^5 &= \omega^6\omega^{-1} = 3(1-2\omega) = 3 - \omega = -2 - \omega \\
\omega^7 &= \omega^6\omega = 3\omega = -2\omega \\
\omega^{11} &= \omega^{12}\omega^{-1} = -(1-2\omega) = -1 + 2\omega \\
\omega^{13} &= \omega^{12}\omega = -\omega \\
\omega^{17} &= \omega^{12}\omega^5 = -(-2-\omega) = 2 + \omega \\
\omega^{19} &= \omega^{12}\omega^7 = -3\omega = 2\omega
\end{aligned}$$

Solution to Question 11 A— constructibility – 11 marks

(a) The ruler assumption is equivalent to starting the construction with the set $S = \{(0,0),(1,0),(\sqrt[6]{2},0)\}$, and squaring a circle with radius $\sqrt{2}$ is equivalent to constructing the point $(\sqrt{2\pi},0)$ out of S.

If this was possible, then, by Theorem 2.7 of Chapter 19, the number $\sqrt{2\pi}$, and hence also $\frac{1}{2}(\sqrt{2\pi})^2 = \pi$, would lie in an extension of $\mathbb{Q}(\sqrt[6]{2})$ of degree a power of 2.

But then, by the KLM Theorem Theorem 2.29 of Chapter 18, the degree $[\mathbb{Q}(\pi):\mathbb{Q}]$ would be finite, a contradiction since π is known to be transcendental over $\mathbb{Q}$.

It follows that it is impossible to square a circle of radius $\sqrt{2}$ with such a ruler (and compasses, of course).

cf. the proof of Theorem 2.11 in Chapter 19

(b) This is equivalent to starting the construction with the points 0, 1 and π^2 on the x-axis of a plane.

It is possible to construct the point $\sqrt{\pi^2} = \pi$ on the x-axis, for example, by the construction described in Figure 2.4 of Chapter 19.

But then 2π is constructible, and the same token as above it is possible to construct the point $\sqrt{2\pi}$ on the x-axis. Hence, it is possible to square a circle of radius $\sqrt{2}$ with this ruler (and compasses).

Figure 2.4 of Chapter 19

(c) Duplication of a unit cube from the set of three points 0, 1 and $\sqrt[3]{4}$ on the x-axis with ruler and compasses is equivalent to constructing the point $\sqrt[3]{2}$ on the x-axis.

Since $\sqrt[3]{4} = (\sqrt[3]{2})^2$, one just needs to take a square root of $\sqrt[3]{4}$, for example, using the construction in Figure 2.4 of Chapter 19.

construction in Figure 2.4 of Chapter 19

(d) Triplication of a unit cube from the set of three points 0, 1 and $\sqrt[6]{3}$ on the x-axis with ruler and compasses is equivalent to constructing the point $\sqrt[3]{3}$ on the x-axis.

Since $\sqrt[3]{3} = (\sqrt[6]{3})^2$, the number $\sqrt[3]{3}$ is constructible, for example, by the construction from Proposition 2.4 (see Figure 2.10) of Chapter 19.

The construction from Proposition 2.4 (see Figure 2.10) of Chapter 19

Solution to Question 11 B— encryption – 11 marks

(a) For $Q = 5P = (4, 0)$ we have $Q = -Q$ and so $10P = \mathcal{O}$, so that the order of P is a positive divisor of 10, greater than 1.

But $5P = (4, 0) \neq \mathcal{O}$ and also $2P \neq \mathcal{O}$ since otherwise we would have $5P = P$, which is not the case. Therefore the order of P in $(E, +)$ is 10.

(b) By (a) the order e of $(E, +)$ is a multiple of 10.

By the inequality of Theorem 2.20 of Chapter 20 with $q = 11$, we have $|e - 12| \leq 2\sqrt{11} < 7$, which implies that $e = 10$.

Since $(E, +)$ has order 10 and contains an element of order 10 we conclude that $(E, +)$ is a cyclic group.

(c) In the notation of Definition 2.9, Lemma 2.10(b) and Definition 2.12 of Chapter 20, we find, for $P = (x_0, y_0) = (0, 4)$ and $a = 2$, $b = 5$ in GF_{11}:

$$c_0 = (3x_0^2 + a)/(2y_0) = 2/8 = 1/4 = 4^{-1} = 3$$
$$d_0 = (-x_0^3 + ax_0 + 2b)/(2y_0) = (2 \cdot 5)/(2 \cdot 4) = 5 \cdot 4^{-1} = 5 \cdot 3 = 4$$
$$x' = c_0^2 - 2x_0 = 9 = -2$$
$$y' = c_0 x' + d_0 = 3 \cdot (-2) + 4 = -2,$$

so that $2P = (x', -y') = (9, 2)$.

(d) By the Diffie-Hellman scheme (cf. Example 2.21 and Exercise 2.7 of Chapter 20) we know that $M_1 = kP = 3P$. Referring to the notation of Definition 2.9, Lemma 2.10(a) and Definition 2.12 of Chapter 20 we find, for $P_1 = 2P = (x_1, y_1) = (9, 2) = (-2, 2)$, $P_2 = P = (0, 4)$, and $a = 2$, $b = 5$ in GF_{11}: $c = (y_2 - y_1)/(x_2 - x_1) = 2/2 = 1$,
$d = (y_1 x_2 - y_2 x_1)/(x_2 - x_1) = 8/2 = 4$, $x_3 = c^2 - x_1 - x_2 = 3$,
$y_3 = cx_3 + d = 1 \cdot 3 + 4 = 7 = -4$, so that $3P = P_1 + P_2 = (x_3, -y_3) = (3, 4)$.

Alice's message is $M = (0, 7) = -P$. By the Diffie-Hellman scheme we have $M_2 = M + kP_B = -P + 3 \cdot 2P = -P + 6P = 5P = (4, 0)$.

See Example 2.21 and Exercise 2.7 of Chapter 20

(e) Bob calculates $M_2 - s_B M_1 = 5P - 2 \cdot 3P = 5P - 6P = -P = (0, 7)$, which is Alice's message.